

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**
*(The requirements of the DoD Industrial Security Manual apply
to all security aspects of this effort.)*

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

Top Secret

b. LEVEL OF SAFEGUARDING REQUIRED

Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

a. PRIME CONTRACT NUMBER

N/A

b. SUBCONTRACT NUMBER

N/A

c. SOLICITATION OR OTHER NUMBER

WISP7T-04-R-L802

DATE (YYYYMMDD)

2004/01/23

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

a. ORIGINAL *(Complete date in all cases)*

DATE (YYYYMMDD)

20040105

b. REVISED
*(Supersedes all
previous specs)*

REVISION NO.

DATE (YYYYMMDD)

c. FINAL *(Complete item 5 in all cases)*

DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT?

☐ YES

☒ NO

Classified material received or generated under

(Previous Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254?

☐ YES

☒ NO

In response to the contractor's request dated

, retention of the classified material is authorized for the period of

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE

Raytheon Company
1501 72nd Street North
St. Petersburg, FL 33710

b. CAGE CODE

00724

c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

Defense Security Service (S4RI)
2500 Leahy Avenue
Orlando, FL 32893-1800

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE

N/A

b. CAGE CODE

N/A

c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

N/A

9. ACTUAL PERFORMANCE

a. LOCATION

Raytheon Company
1501 72nd Street North
St. Petersburg, FL 33710

b. CAGE CODE

00724

c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

Defense Security Service (S4RI)
2500 Leahy Avenue
Orlando, FL 32893-1800

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Support of the Joint Tactical Terminal/Common Integrated Broadcast Service - Modules (JTT/CIBS-M) for Out of Warranty Repair, Field Upgrades, Host Integration Supports, and Studies.

10. CONTRACTOR WILL REQUIRE ACCESS TO:

	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sanctioned Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. NATO INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
k. OTHER <i>(Specify)</i>	<input type="checkbox"/>	<input type="checkbox"/>

SCG & SOW Security Section

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:

	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
i. HAVE TEMPEST REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
l. OTHER <i>(Specify)</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

Reset

12. **PUBLIC RELEASE.** Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

PUBLIC RELEASE OF SCI IS NOT AUTHORIZED

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. **SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (If it is as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidance/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

SEE SECTION 13 CONTINUATION SECTION AT THE BOTTOM

14. **ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract documents itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

SEE SCI ADDENDUM & BLOCK 13

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements covered and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SEE SCI ADDENDUM

16. **CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPE/D NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
CHRISTOPHER J. HARVEY LTC, SC	PRODUCT MANAGER CGS/DI	732-427-5059

d. ADDRESS (Include Zip Code)

PM DCGS-A, SFAR-IUW&S-DCGSA-JTT
BLDG 550 Salzman Avenue
Fort Monmouth, NJ 07703-5304

e. SIGNATURE



17. REQUIRED DISTRIBUTION

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | 1. CONTRACTOR |
| <input type="checkbox"/> | 2. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | 3. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | 4. U.S. ACTIVITY RESPONSIBLE FOR OUTREAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | 5. ADMINISTRATIVE CONTRACTING OFFICE |
| <input checked="" type="checkbox"/> | 6. OTHERS AS NECESSARY |

Continuation of DD 254 Item 13

Contract#:

Solicitation Number: W15P7T-04-R-L802

10a./11h. Accountable COMSEC information/material will be processed IAW DOD 5220.022-S, COMSEC Supplement. Additional Security Guidelines for COMSEC, Appendix G

10e (1)(2). Intelligence Materials Access Required, Appendix H, US Army SCI Addendum to DD Form 254, Appendix I, Contract Monitor (CM)/Alternate Contract Monitor (ACM) Information, Appendix J, SCI Contract Requirement Checklist, Appendix K. SCI Classified information will be protected IAW with the NISPOM, Chapter 5 and the NISPOM Supplement. See Contract monitor's signature block, with signature at bottom of this Block.

10i. Limited Dissemination Information (LIMDIS) require special handling, investigative, or need-to-know functions and are governed by Policy Memorandum, Secretary of the Army, 21 April 1989 and Change , DOD 5200.1R, 27 June 1988.

10j. Safeguarding "FOR OFFICIAL USE ONLY" (FOUO) information, Appendix F.

10k. Enclose attached and dated Security Classification Guide (SCG). Security Considerations is in SOW security section.

11c. The contractor will receive and generate classified documents or other material and will be required to maintain a safeguard capability at their facility IAW NISPOM, Chapter 5.

11d. The contractor is required to provide adequate and approved storage facility for classified hardware material to the level of SECRET. The development effort of the security functions of the JTT/CIBS-M systems shall be accomplished in a restricted area as defined in Paragraph 5-305, DoD 5220.22M, National Industrial Security Program Operating Manual (NISPOM), by contractor personnel cleared at the SECRET level. The following caveat will be stamped on the front and back of all documents that leave the protected area, in addition to appropriate classified marking:

Further Dissemination Only As
Directed by PM DCGS-A, JTT
or Higher DoD Authority

11i. Control of Comprimising Emanations (TEMPEST), Appendix E.

11k. The contracting activity will request DCS services from Commander, DCS, ATTN: Operations Division, Fort George Meade, MD 20755-5370. Guidance for DCS is found in DOD 5200.33, Defense Courier Service Regulation.

Continuation of DD 254 Item 13

Contract#:

Solicitation Number: W15P7T-04-R-L802

13a. Contractor personnel performing ADP (IT) sensitive duties are subject to investigative and assignment requirements IAW AR 380-67 and affiliated regulations.

13b. Classified information will be protected IAW the NISPOM, Chapter 5.

A handwritten signature in black ink, reading "Hung Q. Le". The signature is fluid and cursive, with the first letters of each name being capitalized and prominent.

Hung Q. Le
Contract Monitor

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**
*(The requirements of the DoD Industrial Security Manual apply
to all security aspects of this effort.)*

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

Top Secret

b. LEVEL OF SAFEGUARDING REQUIRED

Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

a. PRIME CONTRACT NUMBER

N/A

b. SUBCONTRACT NUMBER

N/A

c. SOLICITATION OR OTHER NUMBER

W15P7T-04-R-L802

DUE DATE (YYYYMMDD)

2004/01/23

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

a. ORIGINAL *(Complete date in all cases)*

DATE (YYYYMMDD)

20040105

b. REVISED
*(Supersedes all
previous specs)*

REVISION NO.

DATE (YYYYMMDD)

c. FINAL *(Complete Item 5 in all cases)*

DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT?

☒ YES

☐ NO

If Yes, complete the following:

Classified material received or generated under

DAAB07-97-C-J437

(Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254?

☐ YES

☒ NO

If Yes, complete the following:

In response to the contractor's request dated

, retention of the classified material is authorized for the period of

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE

Raytheon Company
1501 72nd Street North
St. Petersburg, FL 33733-2248

b. CAGE CODE

00724

c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

DIS/Director of Industrial Security
2300 Lake Park Drive, Suite 250
Smyrna, GA 30080-7606

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE

N/A

b. CAGE CODE

N/A

c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

N/A

8. ACTUAL PERFORMANCE

a. LOCATION

Raytheon Company
1501 72nd Street North
St. Petersburg, FL 33733-2248

b. CAGE CODE

00724

c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

DIS/Director of Industrial Security
2300 Lake Park Drive, Suite 250
Smyrna, GA 30080-7606

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Support of the Joint Tactical Terminal/Common Integrated Broadcast Service - Modules (JTT/CIBS-M) for Out of Warranty Repair, Field Upgrades, Host Integration Supports, and Studies.

10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. RESTRICTED DATA		<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FORMERLY RESTRICTED DATA		<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>	<input type="checkbox"/>
e. INTELLIGENCE INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY		<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input type="checkbox"/>	<input checked="" type="checkbox"/>
(2) Non-SCI		<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		<input type="checkbox"/>	<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>	<input type="checkbox"/>
g. NATO INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS		<input checked="" type="checkbox"/>	<input type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER <i>(Specify)</i>		<input type="checkbox"/>	<input checked="" type="checkbox"/>
k. OTHER <i>(Specify)</i>							

SCG & SOW Security Section

DD FORM 254, DEC 1999

PREVIOUS EDITION IS OBSOLETE.

Reset

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

PUBLIC RELEASE OF SCI IS NOT AUTHORIZED

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

SEE SECTION 13 CONTINUATION SECTION AT THE BOTTOM

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

SEE SCI ADDENDUM & BLOCK 13

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SEE SCI ADDENDUM

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

CHRISTOPHER J. HARVEY
LTC, SC

b. TITLE

PRODUCT MANAGER CGS/DL

c. TELEPHONE (Include Area Code)

732-427-5059

d. ADDRESS (Include Zip Code)

PM DCGS-A, SFAE-IEW&S-DCGSA-JTT
BLDG 550 Salzman Avenue
Fort Monmouth, NJ 07703-5304

e. SIGNATURE

17. REQUIRED DISTRIBUTION

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR |
| <input type="checkbox"/> | b. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY |

Appendix 1

CONTRACT # W15P7T-04-R-L-802

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

(Provided by the Deputy Chief of Staff for Intelligence (DCSINT))

Contractor Generated COMSEC Material: Any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs and special inspection reports, engineering notes, computations and training aids) will be classified according to its own content. Classification guidance will be taken from other elements of this Contract Security Classification Specification, DD Form 254, Government furnished equipment or data, or special instructions issued by the Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS:

1. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
2. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement "Not Releasable to the Defense Technical Information Center per DOD Directive 5100-38."
3. Classified paper COMSEC material may be destroyed by burning, pulping, or pulverizing. When a method other than burning is used, all residue must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
4. The following downgrading and Declassification notation applies to all classified COMSEC information provided to and generated by the contractor:

DERIVED FROM: NSA/CSSM-123-2

DECLASSIFY ON: Source Marked "OADR" (if generated before 1 April 1995)

DATE OF SOURCE: (Date of document from which information is derived)

5. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the Director, NSA.

Appendix 1

CONTRACT # W15P7T-04-R-L-802

6. Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information without the express written permission of the Director, NSA, is strictly prohibited.

7. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.

8. The requirements of DOD 5220-22-S are applicable to this effort.

9. Additional notices to be affixed to the cover and title or first page of contractor generated COMSEC documents:

a. "COMSEC MATERIAL - ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE."

b. "THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONALS WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA."

10. Point of contact is the DCSINT, AMSEL-MI.

Appendix—2

CONTRACT# W15P7T-04-R-L-802

INTELLIGENCE MATERIALS ACCESS REQUIREMENTS

(Provided by the Deputy Chief of Staff for Intelligence (DCSINT))

1. No Intelligence materials are to be provided in support of the contract without the prior approval of the Intelligence Support Team (IST) (Foreign Intelligence Office), Deputy Chief of Staff for Intelligence (DCSINT), U.S. Army Communications-Electronics Command (USA CECOM). Any intelligence materials so provided will be disseminated solely by the IST, and will be accompanied by both a Letter of Instruction governing control of the materials provided, and a Letter of Transmittal, identifying the materials loaned and the duration of the loan. This service only pertains to elements supported by the Intelligence Support Team, DCSINT, USA CECOM.
2. Point of contact is CECOM DCSINT, AMSEL-MI.

Appendix 3

CONTRACT# W15P7T-04-R-L-802

US ARMY SCI ADDENDUM TO DD FORM 254, 7 June 2002

XXX (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, US Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff for Intelligence (DCSINT), as the Cognizant Security Authority (CSA) for the US Army, has exclusive security responsibility for all SCI released to the contractor or developed under the contract and held within the Contractor's SCI Facility (SCIF) or Co-utilization Agreement (CUA) SCIF. The Defense Intelligence Agency (DIA) has security inspection responsibility for SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under the contract and held within the DOD Contractor's SCIF. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel and information security for safeguarding SCI, and are part of the security classification specification for this contract:

XXX DoD-5105.21-M-1, SCI Security Manual, Administrative Security

XXX DoD TS-5105.21-M-2, SCI Manual, COMINT Policy

 DoD TS-5105.21-M-3, TK Policy

 DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems

 DCID 1/21, Physical Security Standards for Construction of SCIFs

 DIAM 50-4, DoD Intelligence Information System

 DIAM 50-24, Security for Using Communications Equipment in a SCIF

 AR 380-19, Information System Security

XXX AR 380-28, DA Special Security System

 AR 380-381, Special Access Programs (SAPS)

XXX Army Handbook for SCI Contracts

 Other:

XXX (2) Contractor estimated completion date _____ (NOTE: Section "F" of the contract normally provides the Period of Performance. Option years are not to be included as an option is not valid until exercised by the government).

XXX (3) The name, telephone number, e-mail address and mailing address of the Contract Monitor (CM) for the SCI portion of this contract is: (Additionally, identify the Security POC & phone number and e-mail address at the contractor's/subcontractor's location):

XXX (4) All DD Form 254s prepared for subcontracts involving access to SCI under this prime contract must be forwarded to the CM for approval and then to HQ INSCOM, ACoFs Security, G-2, Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

Appendix 3

CONTRACT# W15P7T-04-R-L-802

XXX (5) The contractor will submit the written request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the appropriate Contract Support Element at least ten (10) working days prior to the visit.

XXX (6) The contractor will not reproduce any SCI related material without prior written permission of the CM.

 (7) Security Classification Guides or extracts are attached or will be provided under separate cover.

 (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3, DIAM 50-4 and AR 380-19 (NOTE: Check only if item 11L indicates that a requirement exists for SCI AIS processing).

 (9) This contract requires a contractor SCIF.

XXX (10) This contract requires (SI) (TK) (G) HCS Accesses (add others as required).

 (11) The contractor will perform SCI work under this contract at the following locations:

Appendix 4

CONTRACT# W15P7T-04-R-L-802

SCI
CONTRACT MONITOR (CM)/ALTERNATE CONTRACT MONITOR (ACM)
INFORMATION

Under the provisions of DIAM 50-5, a Contract Monitor must be designated as soon as possible for all SCI Contracts. Appointment orders will be prepared by the Senior Intelligence Officer (SIO) for CECOM/Ft Monmouth. Request the following information be submitted to the Deputy Chief of Staff for Intelligence (DCSINT), ATTN: AMSEL-MI. All appointment orders will then be forwarded to the appropriate activities/personnel.

Appendix 4

CONTRACT# W15P7T-04-R-L-802

CONTRACT MONITOR

ALTERNATE

NAME:

SSN:

ADDRESS (ACTIVITY, OFFICE SYMBOL, BUILDING NO.

(CM) _____

(ACM) _____

TELEPHONE #

DSN (CM): _____

(ACM) _____

COMM (CM): _____

(ACM) _____

CONTRACT COMPANY INFORMATION

CONTRACT NUMBER:

EXPIRATION DATE:

CONTRACT COMPANY NAME AND ADDRESS:

TELEPHONE NUMBER: _____

CAGE CODE: _____

APPENDIX 5

CONTRACT# W15P7T-04-R-L-802

SCI CONTRACT REQUIREMENT CHECKLIST

Appropriate personnel from the user activity, i.e., Project Leader, CM/ACM, Technical Personnel, Contracting Officers, etc., must participate in completing this checklist for all SCI contracts. Some information can be obtained from the CECOM Industrial Security Specialist, DCSINT.

Question	Yes or No Response	Date Completed
1. Obtain a draft statement of work (SOW) and SOW Number		
2. Does the SOW reflect the SCI requirement?		
3. Does the SOW identify the level of classification for Contract? If 'YES', what is the classification level?		
4. Does the SOW identify the need for contractor access to SCI? a. If yes, provide the SCI contract monitor's (CM) name, phone # b. Has the CM/ACM received appropriate training in the duties of administering an SCI contract? (date)		
5. Verify documentation prepared by the SCI CM that supports the need for contractor access to SCI a. Does the documentation fully justify the types of sensitive compartmented information needed, why the contract can't be completed without the access, and how the information will be used? b. Does the draft SOW work reflect the SCI requirements? c. Does the documentation provide estimates of the number of contractor personnel requiring access to SCI? d. What is the projected number of contractor personnel requiring SCI access? e. Has supporting documentation and name of SCI CM been provided to the SIO or appropriate security office for review of SCI requirements and preparation of SCI CM appointments?		
6. Has the approved checklist, supporting documentation and SOW been provided to the Contracting Officer or his/her security representative for preparation of and inclusion in the initial/base DD Form 254?		
7. Has the contract documentation been submitted to the INSCOM Contractor Support Element (CSE), Fort Meade, MD, for review and concurrence?		

SIO/Intelligence Office Approval _____
Date Approved _____

Appendix 6

CONTRACT # W15P7T-04-R-L-802

SAFEGUARDING “FOR OFFICIAL USE ONLY” (FOUO) INFORMATION

Provided by the Deputy Chief of Staff for Intelligence (DCSINT)

1. The “FOR OFFICIAL USE ONLY” marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.

2. Other non-security markings such as “Limited Official Use” and “Official Use Only” are used by non-DOD User Agencies for the same type of information and should be safeguarded and handled in accordance with instructions received from such agencies.

3. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release, to determine whether a significant and legitimate Government purpose is served by withholding the information portions of it.

4. IDENTIFICATION MARKINGS:

a. An unclassified document containing FOUO information will be marked “For Official Use Only” at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion marking will be shown.

b. Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked ‘FOUO.’

c. Any “FOR OFFICIAL USE ONLY” information released to a contractor by a DOD User Agency is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY
DISCLOSURE UNDER THE FOIA. EXEMPTIONS APPLY.

d. Removal of the “FOR OFFICIAL USE ONLY” marking can only be accomplished by the originator or other competent authority. When “FOR OFFICIAL USE ONLY” status is terminated, all known holders will be notified to the extent possible.

Appendix 6

CONTRACT # W15P7T-04-R-L-802

5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.
6. STORAGE: During working hours "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.
7. TRANSMISSION: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent fourth-class mail.
8. DISPOSITION: When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a trash container or as directed by the User Agency.
9. UNAUTHORIZED DISCLOSURE: Unauthorized disclosure of "FOR OFFICIAL USE ONLY" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.
10. Point of contact is the DCSINT, DSN 987-5875, Commercial (732) 532-5875.

Appendix 7

CONTRACT # W15P7T-04-R-L-802

CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Provided by the Security Support Team
Deputy Chief of Staff for Intelligence (DCSINT)
(Updated 23 October 2003)

1. Reference:
 - a. DOD 5220.22-M, National Industrial Security Program Operating Manual, January 1995.
 - b. Confidential Regulation AR 381-14, Technical Counterintelligence (TCI), 30 September 2002 (U).
2. In accordance with guidance referenced above, a TEMPEST Countermeasure Review (TCR) will only be employed where a threat of exploitation exists. A TCR must be performed by a Certified Tempest Technical Authority (CTTA) and be validated by INSCOM TEMPEST elements prior to allocation of Army funds for TEMPEST countermeasures.
3. When electronic equipment is used to process classified information, a completed DA Form 7453 Facility Technical Threat Assessment (FTTA) Worksheet will be completed IAW with Confidential Regulation AR 381-14, Technical Counterintelligence (TCI), 30 September 2002 (U) only if either of the following conditions applies:
 - a. The contractor will use electronic equipment/facilities to process TOP SECRET, SCI, SAP, SIOP, Restricted Data information; or
 - b. The contractor does not maintain complete physical access control of the facility, e.g., the contractor is located in a suite.
4. Complete TEMPEST assessments will be protected at a minimum of "FOR OFFICIAL USE ONLY". A classification is warranted if classified threat information on the facility is included or significant vulnerabilities are identified.

SECURITY CLASSIFICATION GUIDE
FOR
JOINT TACTICAL TERMINAL
(JTT)

ISSUED BY: Project Manager, Distributed Common Ground
System - Army (DCGS-A),
ATTN: SFAE-IEW&S-DCGSA,
Building 550
Fort Monmouth, NJ 07703-5304

APPROVED BY: Commanding General,
U.S. Army Communications-Electronic Command
(USACECOM)
Fort Monmouth, NJ 07703-5000

DATE: 10 Jun 02

PROGRAM NUMBER: None

SUPERSESSSION: Security Classification Guide for the Joint
Tactical Terminal, dated 10 Apr 00

ACTION OFFICER: Mr. Wai Wong
PM DCGS-A, ATTN: SFAE-IEW&S-DCGSA,
Fort Monmouth, NJ 07703-5304
DSN 987-5795 or Commercial (732) 427-5795
E-mail: wai.wong@iews.monmouth.army.mil

DISTRIBUTION STATEMENT:

Distribution authorized to U.S. Government agencies and their contractors for Administrative or Operational Use. Other requests for this document shall be referred to PM DCGS-A, ATTN: SFAE-IEW&S-DCGSA, Fort Monmouth, NJ 07703-5304.

SECTION 1 - GENERAL INFORMATION

1. Purpose: This Security Classification Guide (SCG) provides instructions and guidance on the security classification of information and material pertaining to Joint Tactical Terminal and Common Integrated Broadcast Service - Modules (JTT/CIBS-M) family of equipment, and its program management aspect. This SCG is also applicable for the existing Commanders' Tactical Terminal (CTT) family of equipment that includes the CTT1, CTT2 and CTT3 systems. Only JTT/CIBS-M and JTT-Briefcase are referred throughout this guide unless otherwise stated.
2. Authority: This guide is issued under the authority of AR 380-5. It constitutes authority and may be cited as the basis for classification, regrading, or declassification of information and material concerning the JTT/CIBS-M and CTT equipment, and the intelligence dissemination networks supported by these terminal systems. Changes in classification required by this guide will be made immediately. Information or material identified as classified in this guide is classified by authority of the approving official identified on the title page.
3. Office of Primary Responsibility (OPR): This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to:
Mr. Wai Wong
PM DCGS-A, ATTN: SFAE-IEW&S-DCGSA,
Fort Monmouth, NJ 07703-5304
DSN 987-5795 or Commercial (732) 427-5795
E-mail: wai.wong@IEWS.monmouth.army.mil
4. Questions and Recommendations: Questions concerning the content and interpretation of this guide should be directed to the issuing activity. If the security classifications contained in this guide impose requirements that are impractical, or if current conditions or progress, scientific or technical, or any other factors indicate a need for changes in this guide, completely justified recommendations should be made through appropriate channels to the issuing activity. Pending final decision, the items shall be afforded a degree of protection equivalent to that of the current guidance. All users of this guide are encouraged to assist in maintaining its currency and adequacy. Any over classification or incorrect classification should be brought to the attention of the issuing activity.
5. Reproduction, Extraction and Dissemination: Authorization recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved with JTT and CTT equipment as well as the intelligence dissemination networks supported by these terminal systems, including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR.
6. Public Release: The fact that certain details of information are to be unclassified does not authorize automatic public release. Proposed public releases of unclassified information must be processed through appropriate channels. Within the Department of the Army, the procedures specified in AR 380-5 will apply. Other DOD activities will comply with DOD Directive 5230.9 and applicable service regulations. Defense contractors will comply with DOD 5220.22-M and other contractual requirements. For those agencies under the cognizance of the U.S. Army Materiel Command, all information concerning the JTT will be processed

Appendix 8

Contract # W15P7T-04-R-L-802

for public clearance to Commander, USA Communications-Electronics Command (CECOM), ATTN: AMSEL-EA-PA, Fort Monmouth, NJ 07703-5000, in accordance with AR 380-5, Paragraph 9-2. Material submitted for clearance through the U.S. Army Materiel Command (AMC) will be forwarded to Commander, HQ, AMC, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001, prior to release to the public.

7. Foreign Disclosure: Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in AR 380-10 and National Disclosure Policy NDP-1. If a country with which the Department of Defense has entered into a reciprocal procurement memorandum of understanding or offset arrangement expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation. Each respective network program office controls the disclosure of its intelligence dissemination networks information.

8. Definitions:

AJ	Anti-Jam
AB	Airborne
CCI	Cryptographic Controlled Item
CIBS-M	Common Integrated Broadcast Service - Modules
CODEC	Coder-Decoder
COMSEC	Communications Security
CTT	Commanders' Tactical Terminal
CW	Continuous Wave
ECM	Electronic Countermeasures
ECCM	Electronic Counter-Countermeasures
ERP	Effective Radiated Power
FT	Field Terminal
IBS	Integrated Broadcast Service
IOC	Initial Operational Capability
JCC	JTT Control Client
JTT	Joint Tactical Terminal
JTT-B	Joint Tactical Terminal - Briefcase
LPI	Low Probability of Intercept
LRIP	Low Rate Initial Production
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
OADR	Originating Agency Determination Required
O&O	Operational and Organizational
OPR	Office of Primary Responsibility
ORD	Operational Requirements Document
ROC	Required Operational Capabilities
SDS	Security Data System
SIDS	Secondary Imagery Dissemination System
TADIL-A	Tactical Digital Information Link - A
TADIXS-B	Tactical Data Information eXchange System-B
TDDS	TRAP Data Dissemination System
TDMA	Time Division Multiple Access
TDIMF	Tactical Data Intercomputer Message Format
TIBS	Tactical Information Broadcast Service
TRANSEC	Transmission Security
TRAP	Tactical Related Applications
TRIXS	Tactical Reconnaissance Intelligence eXchange System
USP	User Specific Processor

SECTION 2 - OVERALL EFFORT

System Description: Joint Tactical Terminal (JTT) family terminal and Common Integrated Broadcast Services - Modules (CIBS-M) provide warfighters with tactical intelligence and targeting information. It provides the critical data links to battle managers, intelligence centers, air defenders, fire support elements and aviation nodes across all Services. JTT/CIBS-M allows the war-fighting CINCs, Army, Air Force, Navy, Marine Corps, Special Operations Forces (SOF) and other agency users to access and to exploit the intelligence networks: Tactical Reconnaissance Intelligence eXchange System (TRIXS), Tactical Information Broadcast Service (TIBS), Tactical Related Applications Program (TRAP) Data Dissemination System (TDDS), and Tactical Data Information eXchange System-B (TADIXS-B). JTT-Briefcase also supports Secondary Imagery Dissemination System (SIDS) and TActical Digital Information Link - A (TADIL-A) network operation. The JTT/CIBS-M will provide the required interoperability interfaces. In addition, the JTT/CIBS-M will support the evolving IBS broadcast architecture, including changes to message formats, and transmission protocols. JTT/CIBS-M also supports Demand Assigned Multiple Access (DAMA) in 5 and 25 kHz SATCOM channels and General Purpose Links (GPL) in both LOS and SATCOM modes of operation.

The JTT and CTT are Joint-Service programs with the U.S. Army as the lead procuring agency. General statements regarding the JTT/CIBS-M and CTT equipment and their use by the Army and other Services or Government agencies are unclassified. Any statements revealing details of progress or shortfalls in specific areas of hardware or software, technical or engineering design when those areas are classified, shall be classified at the same level. The JTT and CTT accomplishments which would spur foreign interest in development of countermeasures or redirect areas of emphasis in alternative countermeasure development to render the JTT and CTT equipment less effective or useless in its intended mission environment shall be classified at a minimum of SECRET.

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
1. Identification:				
a. Model Designation	U			
b. Nomenclature	U			
c. Federal Stock Number	U			
d. National Stock Number	U			
e. Names/terminology's	U			
2. Goals, Mission, Purpose	U			
3. Military Applications	U			
4. End Item:				
a. External View	U			
b. Internal View	U			

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
c. Degree of Protection in packaging, storage and transit	U			
d. Photographs	U			
e. System Specifications	U			
f. Test Data and reports	U/C/S	1.5a,g	X-1 X-3	Note 1
g. Equipment Operational Characteristics	U			
h. Training, Operator Maintenance Manuals	U			
i. Operational Requirements Document (ORD)	U			

SECTION 3 - PERFORMANCE AND CAPABILITIES

1. Performance: Broad generalized information concerning system performance is unclassified. When detailed information is associated with specific performance relevant to the architecture and functional capabilities of an intelligence network, the elements will be classified at the minimum levels indicated in other portions of this guide and/or by a related SCG as noted.

2. Capabilities: Capability information, unlike performance data may require classification even when not associated with specific information. When specific capabilities are revealed, classification and/or special intelligence protections may be required. Information which, if collected together, would allow calculation of the ECCM protection level of the systems shall be classified SECRET.

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
1. JTT functional performance and capabilities	U			
2. Frequency range	U			
a. Transmit/Receive sub-bands:				
- TRIXS	U			
- TIBS	U/S	1.5c	X-1	Note 2
- TDDS	U/S	1.5c	X-1	Note 2
- TADIXS-B	U/S	1.5c	X-1	Note 2
- SIDS (JTT-B only)	U/S	1.5c	X-1	Note 2
- TADIL-A (JTT-B only)	U/S	1.5c	X-1	Note 2

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
3. Quantitative levels of ECCM protection	U/S	1.5a	X-3	Note 3
4. Qualitative assessment of applied ECCM technique	U/S	1.5a	X-3	Note 3
5. Qualitative assessment of ECCM performance	U/S	1.5a	X-3	Note 3
6. Synchronization and resynchronization performance	U			
7. Frequency hopping signal processing techniques	U/S	1.5a	X-3	Note 4
8. Performance of ECCM techniques against specific jammers	S	1.5a	X-3	Note 5
9. Specific or estimated jammer range, azimuth, and elevation	S	1.5a	X-3	Note 5
10. JTT System architecture	U			
11. JTT System initialization time	U			
12. Network interoperability and protocols	U			
13. Message delivery time and network connection times	U			
14. Intelligence network related information:				
- TRIXS	U/S	1.5c	X-1	Note 6
- TIBS	U/S	1.5c	X-1	Note 7
- TDDS	U/S	1.5c	X-1	Note 8
- TADIXS-B	U/S	1.5c	X-1	Note 8
- SIDS (JTT-B only)	U/S	1.5c	X-1	Note 15
- TADIL-A (JTT-B only)	U/S	1.5c	X-1	Note 15
15. Message throughput	U			
16. Security level of network data or releasability of network data	U			
17. JTT interfaces to other systems:				
a. The fact that JTT is physically integrated into a specific platform	U			

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
b. The fact that JTT interfaces with specific intelligence broadcasts	U			
18. The fact that JTT can handle the highest classification level of network data	U			
19. Message formats which JTT processes:				
a. Format Name	U			
b. Over-the-air message format/data fields:				
- TRIXS/USMTF	U			
- TRIXS/KEMTI	U			
- TIBS	S	1.5c	X-1	
- TDDS	S	1.5c	X-1	
- TADIXS-B	S	1.5c	X-1	
- SIDS (JTT-B only)	S	1.5c	X-1	Note 15
- TADIL-A (JTT-B only)	S	1.5c	X-1	Note 15
c. Host ICD/TDP ICD	U			
d. Output Intell/contact reports and formats (e.g., TDIMF)	S	1.5c	X-1	
e. Live or Real World Intell Reports	S/TS/SCI	1.5c	X-1	Note 9
20. Internal tamper protection				
a. Purpose/mechanism	U			
b. Detection switch locations	U			
21. Message filtering:				
a. Filtering capability	U			
b. Filter types	U			

SECTION 4 - SPECIFICATIONS

1. Production Characteristics: Specifications which reveal classifiable performance or capabilities information will be classified in accordance with the applicable sections of this guide. Production hardware, standards for qualities of materials and parts, methods or modes of construction, manufacture or assembly and specific dimensions in size, form, shape and weight of the end item are unclassified.

2. Design Information: Complete design specifications which describe the equipment as a whole, or incomplete specifications for component or subsystems from which the design of the equipment as a whole could reasonably be discerned will be unclassified unless elements classified by other portions of this guide are revealed, then the classification will be at the same level of the classified elements.

3. COMSEC Equipment: Specifications for any associated COMSEC equipment and COMSEC requirements will be classified in accordance with guidance provided by the National Security Agency (NSA).

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
1. Ancillary item specifications:				
a. Antenna types and signal gains	U			
b. SATCOM Preamplifier specification	U			
2. Signal acquisition time	U			
3. Channel bandwidth	U			
4. Frequency hopping waveform characteristics	S	1.5a	X-3	
5. Frequency hopping signal structure, pattern, and hop rate	S	1.5a	X-3	
6. Modulation types	U			
7. Data rates	U			
8. COMSEC equipment or embedded crypto	U			
9. Data encryption and encoding techniques and performance	U			
10. Method of synchronization and resynchronization	U			
11. Power supply requirements	U			
12. Environmental Requirements	U			
13. EMI/EMC and TEMPEST Requirements	U			
14. Reliability (MTBF) and Maintainability	U			
15. System Availability (Ao)	U			
16. Transmitter output power requirement	U			
17. Receiver performance:				
a. Sensitivity	U			
b. Dynamic range	U			
c. Input level	U			
d. Bit Error Rate	U			
18. LPI/LPD Requirements	U			

SECTION 5 - CRITICAL ELEMENTS

Not Applicable.

SECTION 6 - VULNERABILITIES AND WEAKNESSES

This section identifies classifications to be assigned to information that discloses inherent weaknesses and vulnerabilities that could be exploited to degrade the system performance or render it useless. General statements of weakness or vulnerability need be classified only when it relates to specific threats against the system. In such cases, classification will be SECRET. When information is associated with intelligence sources and methods, it shall be classified SECRET. Any deficiency (operational vulnerability or spillage of data) discovered should be reported by secure means (SECRET Level) to the issuing agency listed in this Security Classification Guide. The nature of the vulnerability may require special handling. The detailed findings of any investigation may be classified at a higher level than SECRET.

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
1. Vulnerability to ECM				
a. Field Terminal vulnerability to particular types of jammers or jamming scenarios	S	1.5a	X-3	
b. Airborne relay vulnerability to particular types of jammers or jamming scenarios	S	1.5a	X-3	
2. Location of potential jammers against JTT	S	1.5a	X-3	
3. Potential jammers				
a. Power levels	S	1.5a	X-3	
b. Platforms on ground or air	S	1.5a	X-3	
c. Types (pulse, swept, CW, etc.)	S	1.5a	X-3	
d. Antenna gain, and beam-width	S	1.5a	X-3	
e. ERP	S	1.5a	X-3	
4. Quantitative assessment, or measurement, or ECM, or other counter-countermeasure weaknesses of JTT components or the system as a whole	S	1.5a	X-3	

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
5. Test data that indicates JTT susceptibility to specific jammer types and scenarios	S	1.5a	X-3	
6. TEMPEST Test Performance	U/C/S	1.5a	X-3	Note 10
7. Vulnerability to physical attack including directed energy weapons and nuclear, biological or chemical agents	S	1.5a	X-3	

SECTION 7 - ADMINISTRATIVE DATA

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
1. Administrative:				
a. Program office organization	U			
b. Responsibilities	U			
c. Service participation	U			
2. Funding:				
a. Procurement and programming actions that specifies total budget	U			
b. Procurement and programming actions that specify acquisition objective or total program	U			
c. Unit cost associated acquisition objective or total program	U			
3. Production and delivery:				
a. Numbers contracted	U			
b. Production and program schedules	U			
c. Rate of delivery	U			
d. Numbers delivered	U			
4. Key schedules:				
a. IOC/FOC	U			
b. Developmental milestones other than IOC	U			

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
c. Individual test or demonstration dates	U			
d. Future schedule of test and demonstration dates	U			
e. First unit equipped date	U			
f. Phase out date	U			
5. Quantities				
a. Worldwide	U			
b. By theater or command	U			
c. Program quantities for prior budget, and future years	U			
d. Specific quantities of equipment identified for a specific system interface or platform interface	U			
6. Contractor data				
a. Identification of one or more contractors to include prime, associate, or sub	U			
b. Association of an individual contract number with a specific contractor	U			
c. Association of contractor project number or name with Government programs	U			
7. Foreign Military Sales Issues:				
a. Highest level of classified information that could be disclosed by sale of the end item	S	1.5a	X-3	
b. Highest level of classified information that must be disclosed to enable production of the end item	S	1.5a	X-3	

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
c. Highest level of classified information that must be disclosed by operation of the end item	S	1.5a	X-3	
d. Highest level of classified information that must be disclosed in the maintenance of the end item	S	1.5a	X-3	
e. Highest level of classified information that must be disclosed in training to use the end item	S	1.5a	X-3	
f. Highest level of information that could be revealed by reverse engineering the end item	S	1.5a	X-3	
g. Highest classification of information that could be revealed by testing the end item	S	1.5a	X-3	

SECTION 8 - HARDWARE AND SOFTWARE

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
1. Hardware:				
a. JTT-T/R				
- Receiver/Exciter LRU	U/S	1.5c	X-1	Note 11
- High Power Amplifier LRU	U			
b. JTT-R	U/S	1.5c	X-1	Note 11
c. JTT-B				
- Radio Receiver LRU	U/S	1.5c	X-1	Note 11
- Host Laptop PC hard drive	S	1.5c	X-1	Note 14
d. CIBS-M	U/S	1.5c	X-1	Note 12
e. CTT3				
- R/B Processor	U/S	1.5c	X-1	Note 11
- RRT	U			
f. CTT2	U/S	1.5c	X-1	Note 11

Appendix 8
Contract # W15P7T-04-R-L-802

INFORMATION ELEMENT	CLASS	REASON	DECLASS	REMARK
g. CTT1				
- R/B Processor	U/S	1.5c	X-1	Note 11
- RRT	U			
h. RRS	U			
i. RRTS	U			
2. Software:				
a. JTT/CIBS-M software:				
Network message format processing software or CIBS-M				
- Object code or executable code	U			
- Source code	U/S	1.5c	X-1	Note 13
- JCC	U			
b. CTT Message Processor (MP) software	U			
c. CTT User Specific	S	1.5c	X-1	
d. Data filter setting	S	1.5c	X-1	
e. Filter units	U			

SECTION 9 - NOTES

1. Test data will be classified when system vulnerabilities are revealed or when it reveals data classified under sections 3 and 6 of this guide, otherwise test data and test reports are unclassified. Fictitious test data in binary form or format is deemed unclassified.
2. The general operating frequency range or band for each of the intelligence networks is not classified, including sub-range or sub-band for uplink and downlink. Specific operational frequencies for the uplink and downlink of each intelligence network is classified SECRET.
3. General description of the system's ECCM function, or capability, or technique is unclassified. Any statements that the system performance is "degraded" or "affected" by a particular ECM technique or jammer, or that the ECCM features are "ineffective" against a particular ECM technique with further elaboration that reveal the vulnerabilities of the terminals, shall be classified SECRET.
4. The fact that JTT and CTT is capable of frequency hopping using HAVE QUICK II is unclassified. Details concerning HAVE QUICK II algorithms, hop rates, specific frequency tables and its operational usage, may be classified SECRET.
5. Specific assessments or performance ratings of the ECCM capability against certain jammers that directly reveal the system vulnerabilities, are classified SECRET.
6. The fact that the TRIXS architecture associated with Guardrail/Common Sensor (GR/CS), AF Contingency Reconnaissance System (CARS) and/or Navy EP-3 Storyteller System is unclassified, provided no specific intelligence system capabilities or technical parameters are divulged. If capabilities or parameters are divulged, the classification depends on the type of intelligence involved and the appropriate intelligence systems security classification guide. General description of the mission and purpose is unclassified. Details on the producer's collection and reporting capabilities, and/or information of the intelligence data, should be consulted with PM Signal Warfare, ATTN: SFAE-IEW-SW-ACS, Fort Monmouth, NJ 07703-5000, or the corresponding SCG's for Guardrail Common Sensor Systems 1, 2, and 4.
7. General description of the mission and purpose is unclassified, provided no specific intelligence platform system capabilities associated with certain producers or technical parameters are divulged. If capabilities or parameters are divulged, the classification depends on the type of intelligence involved and the appropriate intelligence systems security classification guide. It is recommended that the TIBS SCG, dated 10 October 1994, be consulted for the details on TIBS. POC for TIBS SCG is HQ, Air Intelligence Agency, ATTN: TIBS SMO, Kelly AFB, TX.
8. General description of the mission and purpose is unclassified. The intelligence sources and the dissemination methods may be classified at the TS/SCI level. It is recommended that the TDDS SCG Version 1.0, dated September 1996, be reviewed for all necessary details.

9. Live or real world intelligence reports from the broadcast networks are SECRET as a minimum. Information on the TRIXS network can be up to the TS/SCI level depending on the user mission.
10. The TEMPEST requirement for JTT and CTT is unclassified. However, the TEMPEST guidelines, and the test setup and test reports may be classified at CONFIDENTIAL or SECRET depending on the criteria. At any cases, test reports indicate the vulnerabilities or shortcomings of the system, are classified at SECRET.
11. The individual Line Replaceable Unit (LRU) contains embedded COMSEC crypto, is unclassified Cryptographic Controlled Item (CCI) for transportation or storage when no crypto key is loaded. These LRU's will be handled IAW COMSEC regulations and procedures for accountability. When these LRU's are keyed up with operational crypto material, they must be handled as the same classification level which the crypto key is authorized and so indicated.
12. The CIBS-M hardware modules are unclassified with the exception of the CIBS-M Crypto modules, see Note 11.
13. The source code for the Formatter CIBS-M software module is classified SECRET. The source code for other CIBS-M software modules are unclassified.
14. The JTT-B Host Laptop PC is considered classified SECRET when the classified hard drive is installed.
15. General description of the mission and purpose is unclassified. There are different SIDS and TADIL-A networks exist in the Military System. The intelligence sources and the dissemination methods may be classified at the SECRET level. It is recommended that the respective SCG for these networks be reviewed for all necessary details.

APPENDIX A

REASONS FOR THE DECISION TO CLASSIFY

The reasons for classification relates to the categories or elements of what can be classified as specified in Executive Order 12958, "Classified National Security Information", dated 17 April 1995, Section 1.5, are as follows:

- a. Military plans, weapons systems, or operations.
- b. Foreign government information.
- c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
- d. Foreign relations or foreign activities of the United States, including confidential sources.
- e. Scientific, technological, or economic matters relating to National Security.
- f. United States Government Programs for safeguarding nuclear materials or facilities.
- g. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the National Security.

APPENDIX B

EXEMPTION CATEGORIES FOR DECLASSIFICATION

Declassification is either a date or an event that is 10 years or less from the original classification decision, or an exemption category. When a specific date or event is used, there is no change from existing policy stated in AR 380-5. When a specific date or event within 10 years cannot be established, the following exemption categories in Section 1.6(d) of the Executive Order 12958, "Classified National Security Information", dated 17 April 1995, must be applied. This information will remain classified until reviewed in 25 years for continued classification. The categories of the information that may remain classified beyond ten (10) years are:

- a. X-1 - Reveal an intelligence source, method, or activity, or a cryptologic system or activity.
- b. X-2 - Reveal information that would assist in the development or use of weapons of mass destruction.
- c. X-3 - Reveal information that would impair the development or use of technology within a United States weapon system.
- d. X-4 - Reveal United States Military plans, or national security emergency preparedness plans.
- e. X-5 - Reveal foreign government information.
- f. X-6 - Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than ten (10) years from the date of the original decision.
- g. X-7 - Impair the ability of responsible United States Government officials to protect the President, the Vice President and other individuals for whom protection services, in the interest of national security, are authorized.
- h. X-8 - Violate a statute, treaty, or international agreement.

Appendix E

CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Provided by the Security Support Team
Deputy Chief of Staff for Intelligence (DCSINT)
(Updated 23 October 2003)

1. Reference:

- a. DOD 5220.22-M, National Industrial Security Program Operating Manual, January 1995.
- b. Confidential Regulation AR 381-14, Technical Counterintelligence (TCI), 30 September 2002 (U).

2. In accordance with guidance referenced above, a TEMPEST Countermeasure Review (TCR) will only be employed where a threat of exploitation exists. A TCR must be performed by a Certified Tempest Technical Authority (CTTA) and be validated by INSCOM TEMPEST elements prior to allocation of Army funds for TEMPEST countermeasures.

3. When electronic equipment is used to process classified information, a completed DA Form 7453 Facility Technical Threat Assessment (FTTA) Worksheet will be completed IAW with Confidential Regulation AR 381-14, Technical Counterintelligence (TCI), 30 September 2002 (U) only if either of the following conditions applies:

- a. The contractor will use electronic equipment/facilities to process TOP SECRET, SCI, SAP, SIOP, Restricted Data information; or
- b. The contractor does not maintain complete physical access control of the facility, e.g., the contractor is located in a suite.

4. Complete TEMPEST assessments will be protected at a minimum of "FOR OFFICIAL USE ONLY". A classification is warranted if classified threat information on the facility is included or significant vulnerabilities are identified.

Appendix F

SAFEGUARDING “FOR OFFICIAL USE ONLY” (FOUO) INFORMATION Provided by the Deputy Chief of Staff for Intelligence (DCSINT)

1. The “FOR OFFICIAL USE ONLY” marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.

2. Other non-security markings such as “Limited Official Use” and “Official Use Only” are used by non-DOD User Agencies for the same type of information and should be safeguarded and handled in accordance with instructions received from such agencies.

3. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release, to determine whether a significant and legitimate Government purpose is served by withholding the information portions of it.

4. IDENTIFICATION MARKINGS:

a. An unclassified document containing FOUO information will be marked “For Official Use Only” at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion marking will be shown.

b. Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked ‘FOUO.’

c. Any “FOR OFFICIAL USE ONLY” information released to a contractor by a DOD User Agency is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY
DISCLOSURE UNDER THE FOIA. EXEMPTIONS APPLY.

d. Removal of the “FOR OFFICIAL USE ONLY” marking can only be accomplished by the originator or other competent authority. When “FOR OFFICIAL USE ONLY” status is terminated, all known holders will be notified to the extent possible.

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.

6. STORAGE: During working hours "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.

7. TRANSMISSION: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent fourth-class mail.

8. DISPOSITION: When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a trash container or as directed by the User Agency.

9. UNAUTHORIZED DISCLOSURE: Unauthorized disclosure of "FOR OFFICIAL USE ONLY" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

10. Point of contact is the DCSINT, DSN 987-5875, Commercial (732) 532-5875.

Appendix G

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Contractor Generated COMSEC Material: Any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs and special inspection reports, engineering notes, computations and training aids) will be classified according to its own content. Classification guidance will be taken from other elements of this Contract Security Classification Specification, DD Form 254, Government furnished equipment or data, or special instructions issued by the Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS:

1. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
2. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement "Not Releasable to the Defense Technical Information Center per DOD Directive 5100-38."
3. Classified paper COMSEC material may be destroyed by burning, pulping, or pulverizing. When a method other than burning is used, all residue must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
4. The following downgrading and Declassification notation applies to all classified COMSEC information provided to and generated by the contractor:

DERIVED FROM: NSA/CSSM-123-2

DECLASSIFY ON: Source Marked "OADR" (if generated before 1 April 1995)

DATE OF SOURCE: (Date of document from which information is derived)

5. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the Director, NSA.
6. Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

literature or exhibition of such information without the express written permission of the Director, NSA, is strictly prohibited.

7. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.

8. The requirements of DOD 5220-22-S are applicable to this effort.

9. Additional notices to be affixed to the cover and title or first page of contractor generated COMSEC documents:

a. "COMSEC MATERIAL - ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE."

b. "THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONALS WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA."

10. Point of contact is the DCSINT, AMSEL-MI.

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

Appendix H

INTELLIGENCE MATERIALS ACCESS REQUIREMENTS

1. No Intelligence materials are to be provided in support of the contract without the prior approval of the Intelligence Support Team (IST) (Foreign Intelligence Office), Deputy Chief of Staff for Intelligence (DCSINT), U.S. Army Communications-Electronics Command (USA CECOM). Any intelligence materials so provided will be disseminated solely by the IST, and will be accompanied by both a Letter of Instruction governing control of the materials provided, and a Letter of Transmittal, identifying the materials loaned and the duration of the loan. This service only pertains to elements supported by the Intelligence Support Team, DCSINT, USA CECOM.
2. Point of contact is CECOM DCSINT, AMSEL-MI.

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

Appendix I

US ARMY SCI ADDENDUM TO DD FORM 254, 7 June 2002

XXX (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, US Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff for Intelligence (DCSINT), as the Cognizant Security Authority (CSA) for the US Army, has exclusive security responsibility for all SCI released to the contractor or developed under the contract and held within the Contractor's SCI Facility (SCIF) or Co-utilization Agreement (CUA) SCIF. The Defense Intelligence Agency (DIA) has security inspection responsibility for SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under the contract and held within the DOD Contractor's SCIF. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel and information security for safeguarding SCI, and are part of the security classification specification for this contract:

XXX DoD-5105.21-M-1, SCI Security Manual, Administrative Security

XXX DoD TS-5105.21-M-2, SCI Manual, COMINT Policy

XXX DoD TS-5105.21-M-3, TK Policy

 DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems

 DCID 1/21, Physical Security Standards for Construction of SCIFs

 DIAM 50-4, DoD Intelligence Information System

 DIAM 50-24, Security for Using Communications Equipment in a SCIF

XXX AR 380-19, Information System Security

XXX AR 380-28, DA Special Security System

 AR 380-381, Special Access Programs (SAPS)

XXX Army Handbook for SCI Contracts

 Other:

XXX (2) Contractor estimated completion date 01/31/2009 (Base year contract + 4 years option)

(NOTE: Section "F" of the contract normally provides the Period of Performance. Option years are not to be included as an option is not valid until exercised by the government).

XXX (3) The name, telephone number, e-mail address and mailing address of the Contract Monitor (CM) for the SCI portion of this contract is: CHIRUVOLU, SAVITRI savitri.chiruvolu@iew.s.monmouth.anny.mil, BLDG I210 RM 209 FT MONMOUTH, NJ.

The Security POC & phone number and email address at the contractor's location: Karen A McCree 727-302-2211 karen_a_mccree@raytheon.com

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

XXX (4) All DD Form 254s prepared for subcontracts involving access to SCI under this prime contract must be forwarded to the CM for approval and then to HQ INSCOM, ACoFs Security, G-2, Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

XXX (5) The contractor will submit the written request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the appropriate Contract Support Element at least ten (10) working days prior to the visit.

XXX (6) The contractor will not reproduce any SCI related material without prior written permission of the CM.

XXX (7) Security Classification Guides or extracts are attached.

____ (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3, DIAM 50-4 and AR 380-19 (NOTE: Check only if item 11L indicates that a requirement exists for SCI AIS processing).

____ (9) This contract requires a contractor SCIF.

XXX (10) This contract requires __X__(SI) __X__(TK) _____ (G) HCS Accesses (Approximately 10 SCI billets).

XXX (11) The contractor will perform SCI work under this contract at the following locations: Various meeting locations (CONUS) sponsored by DoD and NSA.

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

Appendix J

SCI
CONTRACT MONITOR (CM)/ALTERNATE CONTRACT MONITOR (ACM)
INFORMATION

Under the provisions of DIAM 50-5, a Contract Monitor must be designated as soon as possible for all SCI Contracts. Appointment orders will be prepared by the Senior Intelligence Officer (SIO) for CECOM/Ft Monmouth. Request the following information be submitted to the Deputy Chief of Staff for Intelligence (DCSINT), ATTN: AMSEL-MI. All appointment orders will then be forwarded to the appropriate activities/personnel.

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

Appendix J (continued)

CONTRACT MONITOR

ALTERNATE

NAME: Ms. Savitri Chiruvolu

Mr. Hung Le

SSN: 144-68-3823

473-94-6459

ADDRESS (ACTIVITY, OFFICE SYMBOL, BUILDING NO.)

(CM): PM DCGS-A, SFAE-IEWS-DCGSA, BLDG 550, FORT MONMOUTH, NJ 07703

(ACM): PM DCGS-A, SFAE-IEWS-DCGSA, BLDG 550, FORT MONMOUTH, NJ 07703

TELEPHONE #

DSN (CM): 987-5920

(ACM): 987-5707

COMM (CM): 732-427-5920

(ACM): 732-427-5707

CONTRACT COMPANY INFORMATION

CONTRACT NUMBER: TBD

EXPIRATION DATE:

CONTRACT COMPANY NAME AND ADDRESS: Raytheon Company, 1501 72nd Street
North, St. Petersburg, FL 33710

TELEPHONE NUMBER:

CAGE CODE: 07724

CONTRACT #
SOLICITATION # W15P7T-04-R-L802

APPENDIX K of DD-254

CONTRACT#
SOLICITATION #: W15P7T-04-R-L802

SCI CONTRACT REQUIREMENT CHECKLIST

Appropriate personnel from the user activity, i.e., Project Leader, CM/ACM, Technical Personnel, Contracting Officers, etc., must participate in completing this checklist for all SCI contracts. Some information can be obtained from the CECOM Industrial Security Specialist, DCSINT.

Question	Yes or No Response	Date Completed
1. Obtain a draft statement of work (SOW) and SOW Number	Yes	Feb 2004
2. Does the SOW reflect the SCI requirement?	Yes	Feb 2004
3. Does the SOW identify the level of classification for Contract? If 'YES', what is the classification level? SCI	Yes	Feb 2004
4. Does the SOW identify the need for contractor access to SCI? a. If yes, provide the SCI contract monitor's (CM) name, phone #: Savitri Chiruvolu, 732-427-5920 b. Has the CM/ACM received appropriate training in the duties of administering an SCI contract? (date) Aug 2003.	Yes Yes	Feb 2004 Feb 2004
5. Verify documentation prepared by the SCI CM that supports the need for contractor access to SCI a. Does the documentation fully justify the types of sensitive compartmented information needed, why the contract can't be completed without the access, and how the information will be used? b. Does the draft SOW work reflect the SCI requirements? c. Does the documentation provide estimates of the number of contractor personnel requiring access to SCI? (10 SCI Billets) d. What is the projected number of contractor personnel requiring SCI access? (10 SCI Billets) e. Has supporting documentation and name of SCI CM been provided to the SIO or appropriate security office for review of SCI requirements and preparation of SCI CM appointments?	Yes Yes Yes Yes Yes	Feb 2004 Feb 2004 Feb 2004 Feb 2004 Feb 2004
6. Has the approved checklist, supporting documentation and SOW been provided to the Contracting Officer or his/her security representative for preparation of and inclusion in the initial/base DD Form 254?	Yes	Feb 2004
7. Has the contract documentation been submitted to the INSCOM Contractor Support Element (CSE), Fort Meade, MD, for review and concurrence?	Yes	Feb 2004

SIO/Intelligence Office Approval _____
Date Approved _____